REMARKS

Claims 5-11 and 15-27 are pending in the present application. Claims 5-11, 15-20, and 25 are amended. Reconsideration of the claims is respectfully requested.

I. 35 U.S.C. § 101

The examiner rejects claims 5-11 and 15-20 under 35 U.S.C. § 101 as directed towards non-statutory subject matter. Applicants have amended the claims accordingly, thereby overcoming the rejection.

II. 35 U.S.C. § 103, Obviousness

The examiner rejects claims 5-11, 15, 18, and 20-27 as obvious over *Yavatkar* et al., Method and System for Diagnosing Network Intrusion, U.S. Patent No. 6,735,702 (May 11, 2004) in view of *Skirmont* et al., Method and Apparatus for Load Apportionment Among Physical Interfaces in Data Routers, U.S. Patent No. 6,553,005 (April 22, 2003). This rejection is respectfully traversed.

As to claims 5-11, 15, 18, and 20-27, the Office Action states:

> *Yavatkar* discloses a computer-implemented method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:
>
> Obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system (watchdog agent) (Column 15, lines 4-17);
>
> Obtaining network information, from network equipment connected to the device, regarding the attack (Column 17, lines 32-51);
>
> Determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information (Column 18, lines 32-53);
>
> And that the entry point is associated with a port (Column 18, lines 19-31);
>
> But do not disclose identifying a physical port associated with the logical port.
>
> *Skirmont*, however, discloses identifying a physical port associated with the logical port (Column 2, lines 6-19). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the logical to physical port mapping of *Skirmont* into the intrusion detection system of *Yavatkar* because it is well known in the art or in order to allow for proper routing table modifications that will prevent

attack traffic from entering the network (*Yavatkar*: Column 21, lines 28-35).

Office Action of July 14, 2005, pp. 3-4.

If the Patent Office does not produce a *prima facie* case of unpatentability, then without more the applicant is entitled to grant of a patent. *In re Oetiker*, 977 F.2d 1443, 1445, 24 U.S.P.Q.2d 1443, 1444 (Fed. Cir. 1992); *In re Grabiak*, 769 F.2d 729, 733, 226 U.S.P.Q. 870, 873 (Fed. Cir. 1985). A prima facie case of obviousness is established when the teachings of the prior art itself suggest the claimed subject matter to a person of ordinary skill in the art. *In re Bell*, 991 F.2d 781, 783, 26 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1993). All limitations of the claimed invention must be considered when determining patentability. *In re Lowry*, 32 F.3d 1579, 1582, 32 U.S.P.Q.2d 1031, 1034 (Fed. Cir. 1994). A proper *prima facie* case of obviousness cannot be established by combining the teachings of the prior art absent some teaching, incentive, or suggestion supporting the combination. *In re Napier*, 55 F.3d 610, 613, 34 U.S.P.Q.2d 1782, 1784 (Fed. Cir. 1995); *In re Bond*, 910 F.2d 831, 834, 15 U.S.P.Q.2d 1566, 1568 (Fed. Cir. 1990).

Regarding claim 5, the amended claim is as follows:

> 5. A computer-implemented method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:
>
> obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system;
>
> obtaining network information, from network equipment connected to the device, regarding the attack;
>
> determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information; and
>
> identifying a physical entry point associated with the logical entry point.

II.A. The Examiner Has Failed To State a Prima Facie Obviousness Rejection of Claim 5

II.A.1. The Proposed Combination Does Not Result in the Invention of Claim 5

The examiner has failed to state a prima facie obviousness rejection because the proposed combination does not show or suggest all of the features of the claimed invention. Specifically, the proposed combination does not show or suggest the claimed features of "determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information."

The examiner asserts otherwise, citing from various portions of *Yavatkar* for the asserted proposition that *Yavatkar* does show or suggest this claimed feature. Primarily, the examiner cites the following portion of *Yavatkar*:

> To report, the bloodhound agent moves across the network to the node of its launch point and provides its findings to the watchdog agent. The bloodhound agent transmits the data it has collected to the watchdog agent using a messaging service. After reporting, the bloodhound agent is destroyed. In an exemplary embodiment, the bloodhound agent provides to the watchdog agent a report indicating the path or paths (or a portion of the path or paths) taken by the attack traffic and, possibly, the source of the attack traffic. The source may be indicated as a gateway allowing access to other networks; in such a case the indicated source is not the originating source of the attack. The path as described by the bloodhound agent comprises links and nodes. Links may be denoted using pairs of port/node combinations. For example, a link may be denoted as the link connecting port "Interface 2" on node 22.49.1.3 to port "Interface 4" on node 22.49.1.7. In alternate embodiments the findings may include other types of information. In an alternate embodiment the bloodhound agent need not move to its launch point to report its findings; for example, it may transmit the information across the network using a messaging service and then self-destruct.

Yavatkar, col. 18, ll. 32-53.

The cited portion of *Yavatkar* does not show or suggest "determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information," as claimed. The cited portion of *Yavatkar* does not show or suggest determining a *logical* entry point of the attack. The bloodhound agent described in *Yavatkar* does search "links" and "nodes," though these terms all refer to physical entry points in the context of *Yavatkar*'s statements. Nowhere does *Yavatkar* describe analyzing logical entry points for an attack. Furthermore, *Skirmont* is silent with respect to this claimed feature. Because neither reference discloses the claimed feature, the proposed combination does not show or suggest all of the features of claim 5.

In addition, the cited portion of *Yavatkar* does not show or suggest using a correlation engine in the manner claimed. Nothing in *Yavatkar* shows or suggest using a correlation engine and nothing in *Yavatkar* could be construed to be a correlation engine. Instead, in the portion of *Yavatkar* that the examiner cites, a bloodhound agent moves across network nodes and to find possible entry points of a network attack. The bloodhound agent then reports its findings to the

watchdog agent, which then may report the findings to a user. This principle is also shown in figure 9 of *Yavatkar*, reproduced below:

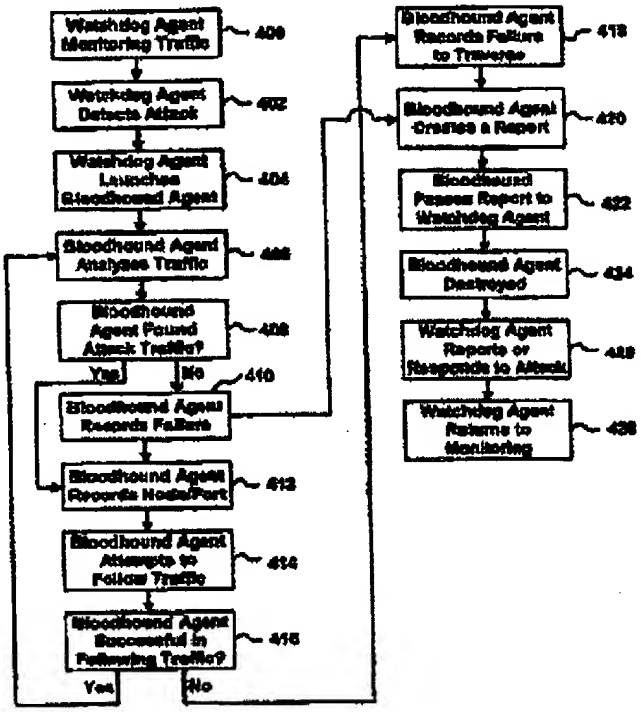

Figure 9

Thus, the bloodhound agent seeks out and individually tests nodes and links in the network for the possible presence of a network attack. The bloodhound agent does not, in any sense, constitute a correlation engine which correlates anything. The bloodhound agent is merely a test and report agent. Similarly, the watchdog agent does not correlate anything. The watchdog agent merely collates information sent by the bloodhound agent and transmits the collated information to a user. Thus, *Yavatkar* does not show or suggest a correlation engine. In addition, *Skirmont* is devoid of disclosure in this regard. Thus, the proposed combination does not show or suggest the claimed feature of using a correlation engine as claimed.

Furthermore, *Yavatkar* does not show or suggest the actual step of "determining a logical entry point of the attack using the correlation engine" as claimed. As shown above, nothing in *Yavatkar* is a correlation engine. Instead, *Yavatkar* individually hunts down points of network attacks by individually testing nodes. This method is less efficient than the claimed method,

which correlates intrusion information and network information to determine a logical entry point of the attack. In addition, *Skirmont* is devoid of disclosure in this regard. For this reason, the proposed combination does not show or suggest this claimed feature.

Still further, *Yavatkar* does not show or suggest the step of "...to correlate the intrusion information and the network information," as claimed. Neither the bloodhound agent nor the watchdog agent correlates intrusion information and network information. While the watchdog information may collate information, a point Applicants do not concede, the watchdog agent does not actually correlate intrusion information and network information. In addition, *Skirmont* is devoid of disclosure in this regard. For this reason, the proposed combination does not show or suggest this claimed feature.

Yavatkar does not show or suggest the claimed feature of "determining a logical entry point of the attack using a correlation engine to correlate the instrusion information and the network information," as claimed. *Skirmont* is devoid of disclosure in this regard. Hence, the proposed combination does not result in the claimed invention and the examiner has failed to state a prima facie obviousness rejection of claim 5.

In addition, the examiner's statement that the entry point is associated with a port appears to be misplaced. The claimed features are as described above. In claim 9, and some other dependent claims, a *logical* port is claimed. A logical port is not the same as a physical port. Thus, the examiner's statement is not understood.

II.A.2. The Examiner Has Failed To State a Proper Motivation To Combine the References Vis-à-Vis Claim 5

The examiner has failed to state a prima facie obviousness rejection against claim 5 because the examiner has failed to state a proper motivation to combine the references. The examiner does not actually state a motivation to combine the references; however, the examiner does state as follows:

> It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the logical to physical port mapping of *Skirmont* into the intrusion detection system of *Yavatkar* because it is well known in the art or in order to allow for proper routing table modifications that will prevent attack traffic from entering the network (*Yavatkar*: Column 21, lines 28-35).

Office Action of July 14, 2005, pp. 3-4.

As a first matter, the statement is not logical vis-à-vis the claimed invention. As shown above, neither *Yavatkar* nor *Skirmont* shows nor suggests determining a logical entry point of the attack using a correlation engine in the manner claimed. For this reason, no one of ordinary skill would logically connect the single relevant fact in *Skirmont* – that those of ordinary skill know that a physical entry point can be associated with a logical entry point – to the method shown in *Yavatkar*. Identifying physical entry points associated with logical entry points has no logical relevance in a reference that does not describe logical entry points and does not use any kind of correlation engine. For this reason, the examiner's statement is not-logical vis-à-vis the claimed invention. Accordingly, the statement cannot serve as a proper motivation to combine the references.

As a second matter, this statement cannot be construed to constitute a proper motivation to combine the references because the statement only asserts that "allowing for proper routing table modifications or in order to allow for proper routing table modifications that will prevent attack traffic from entering the network" is well known in the art. Assuming, arguendo, that the statement is correct, then the examiner has merely pointed out a fact. One of ordinary skill must still have a reason to use this fact to combine the references. The statement does not provide such a reason. Thus, the statement is not a proper motivation to combine the references.

As a third matter, the statement merely describes a purported advantage to combining the references. Assuming, arguendo, that the statement is correct, then an advantage is insufficient to serve as a motivation to combine the references. To constitute a proper motivation, the examiner must establish that one of ordinary skill would both recognize the advantage and have a reason to implement the advantage. For example, a first reference may disclose the use of lasers to achieve nuclear fusion. A second reference may disclose that ultra-high power lasers deliver more energy. One of ordinary skill may recognize that an ultra-high power laser would be more useful to achieve nuclear fusion, though one of ordinary skill would be motivated to avoid combining the references because of the extreme expense of ultra-high power lasers. In this example, one of ordinary skill is motivated to avoid implementing the combination, even if he or she recognized the advantage, and so no motivation exists to combine the references. In the case at hand, the examiner has not provided any reason why one of ordinary skill would have a reason to implement the advantage. For this reason, the examiner's statement fails to provide a proper

motivation to combine the references.

The examiner has failed to state a proper motivation to combine the references because the examiner's statement is illogical vis-à-vis claim 5, because the examiner's statement only points out a purported fact and not a motivation, and because the examiner's statement only points out an advantage, not a motivation. Therefore, the examiner has failed to state a prima facie obviousness rejection of claim 5.

II.A.3. The Examiner Used Impermissible Hindsight When Fashioning the Rejection

The examiner may not use the claimed invention as an "instruction manual" or "template" to piece together the teachings of the prior art so that the invention is rendered obvious. *In re Fritch*, 972 F.2d 1260, 23 U.S.P.Q.2d 1780 (Fed. Cir. 1992). Such reliance is an impermissible use of hindsight with the benefit of applicant's disclosure. *Id.* Therefore, absent some teaching, suggestion, or incentive in the prior art, *Yavatkar* and *Skirmont* cannot be properly combined to form the claimed invention. Absent any teaching, suggestion, or incentive from the prior art to make the proposed combination, the presently claimed invention can be reached only through the an impermissible use of hindsight with the benefit of applicant's disclosure a model for the needed changes.

As shown above, the asserted statement with respect to why it would be obvious to combine the references is not logical vis-à-vis the claimed inventions. Thus, no teaching, suggestion, or incentive from the prior art exists to combine the references. For this reason, the examiner must have simply picked and chosen elements from the art and combined them together using Applicants' disclosure as a template.

In addition, the examiner used a large number of references to find individual elements lacking in several of the dependent claims. This fact emphasizes the fact that the examiner must have simply searched out references with the claimed terms and combined those references with the benefit of hindsight. Picking and choosing elements from the art and combining them using hindsight in this way is impermissible. Therefore, again, the examiner has failed to state a prima facie obviousness rejection of claim 5.

II.B. Claims 6-11, 15, 18, and 20

Claims 6-11, 15, 18, and 20 all depend from claim 5. Therefore, the examiner has failed

to state a prima facie obviousness rejection against these claims at least for the reasons provided above with respect to claim 5.

In addition, these claims contain other features not shown by either reference. For example, neither *Yavatkar* nor *Skirmont* shows nor suggests "wherein the network information includes a *logical* port identifier of a *logical* port associated with the address as claimed." The examiner asserts otherwise, citing the following portion of *Yavatkar*: "In determing which port is accepting the greatest proportion of such traffic...." *Yavatkar*, col. 17, ll. 38-39. However, *Yavatkar* is silent to the claimed feature of a *logical* port.

II.C. The Examiner Has Failed To State a Prima Facie Obviousness Rejection of Claim 25

The examiner has failed to state a prima facie obviousness rejection of claim 25 because the proposed combination does not show or suggest all of the features of claim 25 and because the examiner has failed to state a prima facie obviousness rejection of claim 25. Claim 25 is as follows:

> 25. An apparatus for detecting a point of an attack on a network, the apparatus comprising:
> network equipment for connecting a protected device to a network;
> an intrusion detection system comprising intrusion detection equipment;
> a correlation engine adapted to:
> receive a notification of an attack on the protected device;
> receive intrusion information regarding the attack;
> receive network information regarding the attack, wherein the network information pertains to the network;
> correlate the intrusion information and the network information to produce correlation information;
> use the correlation information to find on the network a logical port of connection used by the attack; and
> map the logical port on the network to a physical port on the network using the correlation engine.

Claim 25 contains features similar to those presented in claim 5. Therefore, the examiner has failed to state a prima facie obviousness rejection of claim 25 at least for the reasons presented with respect to claim 5.

In addition, claim 25 contains the features of "use the correlation information to find on the network a logical port of connection used by the attack" Neither *Yavatkar* nor *Skirmont* show

or suggest these claimed features.

The examiner asserts otherwise, citing column 18, ll. 32-53 of *Yavatkar*. However, as shown above, this portion of *Yavatkar* is devoid of disclosure regarding performing any kind of correlation activity. Certainly, *Yavatkar* does not show using "correlation information" to find on the network a logical port of connection used by the attack. In addition, *Skirmont* is devoid of disclosure in this regard. Therefore, the proposed combination does not show all of the features of claim 25. Accordingly, the examiner has failed to state a prima facie obviousness rejection of claim 25.

In addition, the examiner has failed to state a proper motivation to combine the references. The examiner's statement vis-à-vis claim 25 is substantially the same as the statement vis-à-vis claim 5. Thus, the examiner's statement regarding claim 25 is not a proper motivation to combine the references for he same reason that the examiner's statement regarding claim 5 is not a proper motivation to combine the references.

The proposed combination does not show all of the features of claim 25. Therefore, the proposed combination does not result in the invention of claim 25. In addition, the examiner has failed to state a proper motivation to combine the references. Accordingly, the examiner has failed to state a prima facie obviousness rejection of claim 25.

II.D. Claims 21-24, 26 and 27

Independent claim 21 contains features similar to those contained in claim 25. Therefore, the examiner has failed to state a prima facie obviousness rejection against claim 21 at least for the reasons described above with respect to claim 25. In addition, claims 22-24 depend from claim 21 and claims 26 and 27 depend from claim 25. Therefore, the examiner has failed to state a prima facie obviousness rejection against these claims at least by virtue of their dependence on claims 21 and 25.

In addition, these dependent claims contain other features not shown by either reference. For example, neither *Yavatkar* nor *Skirmont* shows or suggests that the network information includes a *logical* port identifier of a *logical* port associated with the address, as claimed in claim 24. Therefore, the examiner has failed to state a prima facie obviousness rejection of this claim, as well.

II.E. The Claims Are Non-Obvious in View of the References When the References Are Considered as a Whole

In addition, the claims are non-obvious in view of *Yavatkar* and *Skirmont* because these references are directed to solving different problems. *Yavatkar* is directed to solving problems with finding attacks on a network, as shown below:

> Diagnosing network attacks may thus require the distributed state of the network to be known--e.g., what type of traffic is being received at which devices and through which ports, and the path or paths taken by the traffic. Certain information about the state of a network may only be gathered accurately and quickly at the individual nodes distributed throughout a network--for example, the particular port receiving a certain type of attack traffic. Currently, gathering such information requires that an operator physically access individual nodes, e.g., by using a sniffer, or that a central console query remote nodes. Such methods are slow, inefficient and inaccurate. The time taken to perform current diagnosis operations results in inaccuracy, as the state of a network is determined over a period of time. Delays may also occur, if (as may happen during a network attack), data transmission over links is interrupted or halted. The state of a network is not always accurately viewed from one central point which has only indirect access to the state of remote network nodes. Evidence of the source of attack traffic exists with greater certainty nearer the source of the traffic.
>
> Therefore there exists a need for a system and method allowing for the distributed state of a network, such as information about attack traffic, to be quickly and accurately collected. A system and method are needed for quickly and accurately diagnosing network attacks by determining information such as the source of, or a partial path of, attack traffic.

Yavatkar, col. 1, ll. 23-50.

In contrast, *Skirmont* is directed to the problem of determining which of actually physical egress ports to use in a router, as shown below:

> In current art when a packet is received at a router the packets headers are read and typically a forwarding table is consulted to determine the next hop for the packet. This next hop table contains, among other things, the identity of the egress interface to be used and how to send the packet internally to that location. A problem in current art is that the egress interface may well be a defined interface comprising several actual physical egress ports. The problem then is one of determining which of the actual physical egress ports to use. One solution is to simply do another software table lookup. This is not difficult for software based routing elements, but is less than ideal for a high-speed hardware based solution where memory space and ASIC pins may well be limited.

> What is clearly needed for the new generation of very high-speed and more sophisticated routers is a method and system for mapping IP packets that have common source and destination by strict physical paths, while at the same time accomplishing efficient load balancing along the same physical paths.

Skirmont, col. 2, ll. 6-25.

The problems addressed by *Skirmont* and *Yavatkar* are distinct. *Yavatkar* is directed to detecting attacks on networks, whereas *Skirmont* is directed to mapping IP packets by strict *physical* path while simultaneously accomplishing load balancing along the same physical path. The two problems have nothing to do with each other and the solutions to the problems have nothing to do with each other. Because the references are directed toward different problems, one of ordinary skill would have no reason to look to *Skirmont* for the problem addressed by *Yavatkar*. Hence, no motivation exists to combine the references. Accordingly, the claims are non-obvious in view of *Yavatkar* and *Skirmont* when the references are considered as a whole.

II.F. Summary of Flaws in Rejection of Claims 5-11, 15, 18, and 20-27

The examiner failed to state a prima facie obviousness rejection of claims 5-11, 15, 18, and 20-27 because the proposed combination does not show all of the features of the claimed inventions, because the examiner failed to provide a proper motivation to combine the references, and because the examiner used impermissible hindsight when fashioning the obviousness rejections. In addition, these claims are also non-obvious in view of the references when the references are viewed as a whole because no one of ordinary skill would combine references that address wholly different problems as *Yavatkar* and *Skirmont*. Therefore, the rejection of claims 5-11, 15, 18, and 20-27 under 35 U.S.C. § 103 has been overcome.

III. <u>35 U.S.C. § 103, Obviousness</u>

The examiner rejects claim 16 as obvious over *Yavatkar* in view of *Skirmont* further in view of *ND* ("Network Dispatcher: a connection router for scalable Internet services", 10/2/1998, Internet Security Systems, obtained from the cited Web site (hereinafter "*ND*"). This rejection is respectfully traversed.

As to claim 16, the Office Action states:

> *Yavatkar* as modified by *Skirmont* does not disclose that the network equipment includes a network dispatcher.
>
> *ND*, however, discloses that the network equipment includes a network dispatcher (Pages 1-2, Introduction, Paragraphs 1-4). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the network dispatcher of *ND* into the intrusion detection system of *Yavatkar* as modified by *Skirmont* in order to spread the load of the network evenly upon multiple servers or nodes of the network.

Office Action of Jul. 14, 2005, p. 8.

Claim 16 is as follows:

> 16. The computer-implemented method of claim 5, wherein the network equipment includes a network dispatcher.

The rejection is predicated upon the flawed rejection of claim 5 in view of *Yavatkar* and *Skirmont*. Therefore, the examiner has failed to state a prima facie obviousness rejection of claim 16, at least for the reasons presented with respect to claim 5.

In addition, the examiner used a large number of references to find individual elements lacking in several of the dependent claims. This fact emphasizes the fact that the examiner must have simply searched out references with the claimed terms and combined those references with the benefit of hindsight. Picking and choosing elements from the art and combining them using hindsight in this way is impermissible. Therefore, again, the examiner has failed to state a prima facie obviousness rejection of claim 16

In addition, claim 16 is non-obvious in view of the cited references because the references address different problems. *Yavatkar* is directed to solving problems with finding attacks on a network, as described above. In contrast, *Skirmont* is directed to the problem of determining which of actually physical egress ports to use in a router, as described above. The problems addressed by *Skirmont* and *Yavatkar* are distinct. *Yavatkar* is directed to detecting attacks on networks, whereas *Skirmont* is directed to mapping IP packets by strict *physical* path while simultaneously accomplishing load balancing along the same physical path. In further contrast, the *ND* reference is directed to load balancing, as follows:

> As the Web matures, the ability to react to load imbalances becomes increasingly important. Initially, most Web servers delivered content based on more or less uniformly small files. Consequently, if the number of requests was evenly distributed, the load on the servers would be relatively uniform. However, today, and increasingly in the future, Web

> servers hand out more dynamically-generated results with substantial graphics content and a wide variation in the computation required to produce the results. This variation of content and effort makes it much more difficult to keep a group of servers evenly loaded.

ND, p. 2.

The three problems are unrelated and the solutions to the problems have nothing to do with each other. Because the references are directed toward different problems, one of ordinary skill would have no reason to look to *ND* for the problem addressed by *Yavatkar* or *Skirmont*. Hence, no motivation exists to combine the references. Accordingly, the claims are non-obvious in view of *ND*, *Yavatkar*, and *Skirmont* when the references are considered as a whole.

IV. 35 U.S.C. § 103, Obviousness

The examiner rejects claim 17 as obvious over *Yavatkar* in view of *Skirmont* further in view of *Shanklin* et al., Parallel Intrusion Detection Sensors with Load Balancing for High Speed Networks, U.S. Patent No. 6,578,147 (June 10 2003) (hereinafter *Shanklin*). This rejection is respectfully traversed.

As to claim 17, the Office Action states:

> *Yavatkar* as modified by *Skirmont* does not disclose that the network equipment includes a load balancer.
>
> *Shanklin*, however, discloses that the network equipment includes a load balancer (Column 7, lines 39-47). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the load balancer of *Shanklin* into the intrusion detection system of *Yavatkar* as modified by *Skirmont* in order to distribute traffic so that each intrusion detection agent processes only a portion of the traffic.

Office Action of Jul. 14, 2005, pp. 8-9.

Claim 17is as follows:

> 17. The computer-implemented method of claim 5, wherein the network equipment includes a load balancer.

The rejection is predicated upon the flawed rejection of claim 5 in view of *Yavatkar* and *Skirmont*. Therefore, the examiner has failed to state a prima facie obviousness rejection of claim 17, at least for the reasons presented with respect to claim 5.

In addition, the examiner used a large number of references to find individual elements lacking in several of the dependent claims. This fact emphasizes the fact that the examiner must

have simply searched out references with the claimed terms and combined those references with the benefit of hindsight. Picking and choosing elements from the art and combining them using hindsight in this way is impermissible. Therefore, again, the examiner has failed to state a prima facie obviousness rejection of claim 17

In addition, claim 17 is non-obvious in view of the cited references because the references address different problems. *Yavatkar* is directed to solving problems with finding attacks on a network, as described above. In contrast, *Skirmont* is directed to the problem of determining which of actually physical egress ports to use in a router, as described above. The problems addressed by *Skirmont* and *Yavatkar* are distinct. *Yavatkar* is directed to detecting attacks on networks, whereas *Skirmont* is directed to mapping IP packets by strict *physical* path while simultaneously accomplishing load balancing along the same physical path. In further contrast, *Shanklin* is directed to load balancing in intrusion detection systems, as follows:

> One aspect of the invention is a method of detecting unauthorized access on a network as indicated by signature analysis of packet traffic on the network. A plurality of intrusion detection sensors are connected at a network entry point associated with an internetworking device, such as a router or switch. The packet load to the sensors is "load balanced", such that said packets are distributed at least at a session-based level. The load balancing may be at a lower (packet-based) level, which tends to more evenly distribute the load on each sensor but requires additional processing external to the sensors or requires sharing of session-level data between sensors. The sensors are used to detect signatures indicated by the packets. Packets indicating a composite signature from multiple sessions are delivered to a network analyzer, which detects the composite signatures. The results of the detection performed by the sensors and the network analyzer are used to determine if there is an attempt to gain unauthorized access to the network.

Shanklin, col. 1, l. 63 through col. 2, l. 13.

The three problems are unrelated and the solutions to the problems have nothing to do with each other. Because the references are directed toward different problems, one of ordinary skill would have no reason to look to *Shanklin* for the problem addressed by *Yavatkar* or *Skirmont*. Hence, no motivation exists to combine the references. Accordingly, the claims are non-obvious in view of *Shanklin*, *Yavatkar*, and *Skirmont* when the references are considered as a whole.

V. **35 U.S.C. § 103, Obviousness**

The examiner rejects claim 19 as obvious over *Yavatkar* in view of *Skirmont* further in view of *NVHIDS* ("Network- vs. Host-based Intrusion Detection," April 1998, Proceedings of the 7th International World Wide Web conference (WWW7), obtained from documents.iss.net/whitepapers/nvh_ids.pdf) (hereinafter *NVHIDS*). This rejection is respectfully traversed.

As to claim 19, the Office Action states:

> *Yavatkar* as modified by *Skirmont* does not disclose that the intrusion detection system includes host based intrusion detection equipment.
>
> *NVHIDS*, however, discloses that the intrusion detection system includes host based intrusion detection equipment (Page 9, Paragraph 1). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the host based intrusion detection of *NVHIDS* into the intrusion detection system of *Yavatkar* as modified by *Skirmont* in order to improve network resistance to attacks and misuse, enhance enforcement of security policy, and introduce greater flexibility in deployment options.

Office Action of Jul. 14, 2005, p. 9.

Claim 19 is as follows:

> 19. The computer-implemented method of claim 5, wherein the intrusion detection system includes host based intrusion detection equipment.

The rejection is predicated upon the flawed rejection of claim 5 in view of *Yavatkar* and *Skirmont*. Therefore, the examiner has failed to state a prima facie obviousness rejection of claim 19, at least for the reasons presented with respect to claim 5.

In addition, the examiner used a large number of references to find individual elements lacking in several of the dependent claims. This fact emphasizes the fact that the examiner must have simply searched out references with the claimed terms and combined those references with the benefit of hindsight. Picking and choosing elements from the art and combining them using hindsight in this way is impermissible. Therefore, again, the examiner has failed to state a prima facie obviousness rejection of claim 19

In addition, claim 19 is non-obvious in view of the cited references because the references address different problems. *Yavatkar* is directed to solving problems with finding attacks on a

network, as described above. In contrast, *Skirmont* is directed to the problem of determining which of actually physical egress ports to use in a router, as described above. The problems addressed by *Skirmont* and *Yavatkar* are distinct. *Yavatkar* is directed to detecting attacks on networks, whereas *Skirmont* is directed to mapping IP packets by strict *physical* path while simultaneously accomplishing load balancing along the same physical path. In further contrast, *NVHIDS* is directed to describing host-based intrusion detection equipment, as follows:

> Both network- and host-based IDS solutions have unique strengths and benefits that complement each other. A next-generation IDS, therefore, must include tightly integrated host and network components. Combining these two technologies will greatly improve network resistance to attacks and misuse, enhance the enforcement of security policy and introduce greater flexibility in deployment options.
>
> The graphic below illustrates how network- and host-based intrusion detection techniques interact to create a more powerful network defense. Some events are detectable by network means only. Others that are detectable only at the host. Several require both types of intrusion detection to function properly.

NVHIDS, p.9.

The three problems are unrelated and the solutions to the problems are unrelated. Because the references are directed toward different problems, one of ordinary skill would have no reason to look to *NVHIDS* for the problem addressed by *Yavatkar* or *Skirmont*. Hence, no motivation exists to combine the references. Accordingly, the claims are non-obvious in view of *NVHIDS*, *Yavatkar*, and *Skirmont* when the references are considered as a whole.

VI. Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance.

The examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: October 13, 2005

Respectfully submitted,

Theodore D. Fay III
Reg. No. 48,504
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorney for Applicants